

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

In re Patent Application of)	Mail Stop Appeal Brief - Patents
Marc Joye)	
Application No.: 10/537,300)	Group Art Unit: 2431
Filed: June 2, 2005)	Examiner: Longbit Chai
For: METHOD FOR SECURE INTEGER)	Confirmation No.: 1466
DIVISION OR MODULAR)	
REDUCTION AGAINST HIDDEN)	
CHANNEL ATTACKS)	

APPELLANT'S OPENING BRIEF

Mail Stop Appeal Brief - Patents

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This appeal is from the decision of the Examiner in the Final Office Action dated September 2, 2008 and maintained in the Advisory Action dated December 16, 2008 and the Notice of Panel Decision from Pre-Appeal Brief Review dated April 13, 2009. Appellant filed a Notice of Appeal on March 2, 2009.

The Commissioner is hereby authorized to charge any appropriate fees under 37 C.F.R. §§ 1.16, 1.17, and 1.21 that may be required, and to credit any overpayment, to Deposit Account No. 02-4800.

I. REAL PARTY IN INTEREST

The real party in interest is Gemalto, a French corporation, the assignee of Appellant's entire right, title and interest in this application.

II. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences within the meaning of 37 C.F.R. § 41.37(c)(1)(ii) known to Appellant or the undersigned counsel.

III. STATUS OF CLAIMS

Claims 1-8 (reproduced in the attached Appendix), which are under final rejection, are pending in this application.

Claims 1, 2 and 5-8 stand finally rejected under 35 U.S.C. § 102(e) as anticipated by Drexler U.S. Patent Pub. No. 2003/0079139.

Claims 3 and 4 stand finally rejected under 35 U.S.C. § 103(a) as unpatentable over Drexler and Falk U.S. Patent No. 5,077,793.

Claims 1-8 are on appeal.

IV. STATUS OF AMENDMENTS

There are no pending amendments to the appealed claims.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Exemplary embodiments encompassed by Appellant's claims are directed to a method of integer division or modular reduction secure against covert channel attacks, and in particular, differential attacks. The exemplary embodiments can be

used for performing operations in a more general cryptographic method, for example, a secret or public key cryptographic method. Such a cryptographic method can be implemented in electronic devices, such as chip cards, for example.

A mapping of claims 1 and 7 to the disclosure in exemplary sections of Appellant's specification is provided in the following tables.

Claim	Disclosure
1. A cryptographic method during which an integer division of a type $q = a \text{ div } b$ and/or a modular reduction of a type $r = a \text{ mod } b$ is performed, where q is a quotient, a is a number containing m bits, b is a number containing n bits, with n less than or equal to m and b_{n-1} is non-zero, b_{n-1} being the most significant bit of the number b , comprising the steps of masking the number a by a random number p before performing the integer division and/or the modular reduction, and	page 8, line 26 - page 9, line 6
generating encrypted or decrypted data in accordance with a result of the division and/or modular reduction.	page 8, line 26 - page 9, line 6; page 9, lines 12-16; data item a is encrypted or decrypted
7. An electronic component comprising	
means for implementing a method according to claim 1, said means comprising a plurality of registers for storing the numbers a and b .	page 1, lines 10-12; method can be implemented in electronic devices such as a chip card; page 10, lines 15-22; electronic component comprises several registers for storing numbers a and b

VI. GROUND OF REJECTION TO BE REVIEWED ON APPEAL

Appellant requests review of the following grounds of rejection:

A. Whether claims 1, 2 and 5-8 are anticipated under 35 U.S.C. § 102(e) by Drexler U.S. Patent Pub. No. 2003/0079139.

B. Whether claims 3 and 4 are unpatentable under 35 U.S.C. § 103(a) over Drexler and Falk U.S. Patent No. 5,077,793.

VII. ARGUMENT

**A. THE EXAMINER IMPROPERLY REJECTED CLAIMS 1, 2 AND 5-8
AS ANTICIPATED UNDER 35 U.S.C. § 102(e) BY DREXLER
U.S. PATENT PUB. NO. 2003/0079139.**

The Examiner erred in rejecting claims 1, 2 and 5-8 under 35 U.S.C. § 102(e) over Drexler U.S. Patent Pub. No. 2003/0079139.

As set forth in MPEP § 2131, to anticipate a claim, the reference must teach every element of the claim. *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631 (Fed. Cir. 1987). The United States Court of Appeals for the Federal Circuit recently emphasized that "unless a reference discloses within the four corners of the document not only all of the limitations claimed but also all of the limitations arranged or combined in the same way as recited in the claim, it cannot be said to prove prior invention of the thing claimed and, thus, cannot anticipate under 35 U.S.C. § 102." *Net MoneyIN, Inc. v. VeriSign, Inc.*, 545 F.3d 1359, 1371 (Fed. Cir. 2008) (emphasis added).

Appellant respectfully submits that the rejection does not meet this requirement because the Office has not established that Drexler teaches every element of the claims arranged or combined in the same way as recited in the claims.

For example, Appellant's claim 1 recites a cryptographic method during which an integer division of a type $q = a \div b$ and/or a modular reduction of a type $r = a \bmod b$ is performed, where q is a quotient, a is a number containing m bits, b is a number containing n bits, with n less than or equal to m and b_{n-1} is non-zero, b_{n-1} being the most significant bit of the number b , comprising the steps of masking the number a by a random number p before performing the integer division and/or the

modular reduction, and generating encrypted or decrypted data in accordance with a result of the division and/or modular reduction.

According to an exemplary embodiment, the number a can be masked by a random number p before performing the integer division and/or the modular reduction. With the number a being masked by a random number, the trace, for example, the energy consumption, left during the execution of the method can be different at each execution, so that it is no longer possible to implement a differential covert channel attack. The random number p can be modified at each execution of the method, or simply after a predefined number of executions of the method.

Appellant respectfully submits that this same combination of features is neither disclosed nor suggested by Drexler. For example, paragraphs [0004] and [0007] in Drexler are cited for allegedly disclosing the claimed "cryptographic method during which an integer division of a type $q = a \text{ div } b$ and/or a modular reduction of a type $r = a \text{ mod } b$ is performed, where q is a quotient, a is a number containing m bits, b is a number containing n bits, with n less than or equal to m and b_{n-1} is non-zero, b_{n-1} being the most significant bit of the number b ." Appellant respectfully disagrees.

First, paragraph [0004] in Drexler merely states that methods are known that allow a person monitoring the current consumption or timing of the encryption process to deduce secret data, in particular, a secret key. Nothing in paragraph [0004] in Drexler reads on Appellant's claims; rather, Appellant's claims solve this problem. Second, paragraph [0007] in Drexler discloses that it is known for a factor $r \cdot n$ (random number * modulus) to be added for the encryption of the message. The encrypted text $Y = M^d \text{ mod } n$ is thus changed to $(M + r \cdot n)^d \text{ mod } n$, where M is a known message.

However, even when paragraphs [0004] and [0007] in Drexler are combined, the rejection lacks the specificity required under 35 U.S.C. § 102 to establish that these sections of Drexler teach every element of the claimed "cryptographic method during which an integer division of a type $q = a \div b$ and/or a modular reduction of a type $r = a \bmod b$ is performed, where q is a quotient, a is a number containing m bits, b is a number containing n bits, with n less than or equal to m and b_{n-1} is non-zero, b_{n-1} being the most significant bit of the number b " arranged or combined in the same way as recited in the claim.

Next, paragraph [0020] in Drexler is cited for allegedly disclosing the claimed "masking the number a by a random number p before performing the integer division and/or the modular reduction." Appellant respectfully disagrees.

Paragraph [0020] in Drexler recites:

According to the invention, a random number r is first of all chosen, and the product $r*n$ is formed, for the encryption process. The exponentiation process then starts with a squaring operation, in which the product $r*n$ is added to the intermediate result Z in order to calculate the expression $(Z*(Z+r*n) \bmod k*n)$, where k is an integer, instead of $Z*Z \bmod n$. In the situation where the exponent, that is to say the secret key d , contains a "1" at that point, this is followed by a multiplication operation for which, first of all, $(r_i * n)$ is added to the message M , that is to say $M+r_i * n$ is formed and $(Z*(M+r_i * n) \bmod k*n)$ is calculated instead of $Z*M \bmod n$. The process passes through this loop until all the digits in the secret key have been processed, with i being incremented by 1 for the next multiplication process in each case. The result is also mod n reduced after completion of an exponentiation process.

In Appellant's claim, where $r = a \bmod b$, where b is the modulus, number a is masked by a random number p before performing the integer division and/or the modular reduction. In contrast, as noted above in paragraph [0020] in Drexler, random number r is multiplied by the modulus n . Thus, Drexler similarly fails to teach or suggest this element of claim 1 arranged or combined in the same way as recited in the claim.

Paragraph [0005] in Drexler is cited as allegedly disclosing the claimed "generating encrypted or decrypted data in accordance with a result of the division and/or modular reduction" (emphasis added). Appellant again respectfully disagrees.

Paragraph [0005] in Drexler discloses a type of attack ("Simple Power Analysis" (SPA) method), where the encrypted text $Y=M^d \bmod n$ is formed. During the modular exponentiation process, a squaring operation is carried out with the intermediate result and a multiplication operation is carried out with M if there is a "1" in the exponent d, while only a squaring operation with the intermediate result is carried out if there is a "0" in d. If M is known, the times at which the message M is used can be identified by observing the current response and/or the timing during the operations. Since this message is always used if a "1" is present in d, the key can be deduced without any problems.

However, since the claimed division and/or modular reduction is arrived at by masking the number a by a random number p before performing the integer division and/or the modular reduction, and since paragraph [0005] in Drexler does not teach or suggest this feature, the rejection of claim 1 should be withdrawn for this reason as well.

Accordingly, Drexler fails to disclose every element of claim 1 arranged or combined in the same way as recited in the claim. Thus, claim 1 is allowable. This logic also disposes of the rejection of claims 2 and 5-8, which depend from claim 1 and add further distinguishing features.

In view of the above, the Examiner erred in rejecting claims 1, 2 and 5-8 under 35 U.S.C. § 102(e) over Drexler.

B. THE EXAMINER IMPROPERLY REJECTED CLAIMS 3 AND 4 AS UNPATENTABLE UNDER 35 U.S.C. § 103(a) OVER DREXLER AND FALK U.S. PATENT NO. 5,077,793.

The Examiner erred in rejecting claims 3 and 4 under 35 U.S.C. § 103(a) over Drexler and Falk U.S. Patent No. 5,077,793.

Claims 3 and 4 depend directly or indirectly from claim 1 and recite further distinguishing features and are thus also allowable because Drexler is cited for teachings it does not provide. Additionally, Falk, which is cited only for the use of modular subtractors to subtract pseudo-random number sequences from a converted encrypted signal, does not cure the deficiencies of Drexler.

The failure of an asserted combination to teach or suggest each and every feature of a claim remains fatal to an obviousness rejection under 35 U.S.C. § 103, despite any recent revision to the Manual of Patent Examining Procedure (MPEP).

Section 2143.03 of the MPEP requires the “consideration” of every claim feature in an obviousness determination. To render claims 3 and 4 unpatentable, however, the Office must do more than merely “consider” each and every feature for this claim. Instead, the asserted combination of the Drexler and Falk documents must also teach or suggest *each and every claim feature*. See *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974) (emphasis added) (to establish *prima facie* obviousness of a claimed invention, all the claim features must be taught or suggested by the prior art).

Indeed, as the Board of Patent Appeals and Interferences has recently confirmed, a proper obviousness determination requires that an Examiner make “a searching comparison of the claimed invention – *including all its limitations* – with the

teaching of the prior art.” See *In re Wada and Murphy*, Appeal 2007-3733, citing *In re Ochiai*, 71 F.3d 1565, 1572 (Fed. Cir. 1995) (emphasis in original).

Further, the necessary presence of all claim features is axiomatic, since the Supreme Court has long held that obviousness is a question of law based on underlying factual inquiries, including ... ascertaining the differences between *the claimed invention* and the prior art. *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966) (emphasis added). Indeed, Appellant submits that this is why Section 904 of the MPEP instructs Examiners to conduct an art search that covers “the invention *as described and claimed*.” (emphasis added).

Lastly, Appellant respectfully invites the Board's attention to MPEP § 2143, the instructions of which buttress the conclusion that obviousness requires at least a suggestion of all of the features of a claim, since the Supreme Court in *KSR* stated that “there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.” *KSR*, 127 S. Ct. at 1741 (*quoting In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)).

In sum, it remains well-settled law that obviousness requires at least a suggestion of all of the features in a claim. See *In re Wada and Murphy*, citing *CFMT, Inc. v. Yieldup Intern. Corp.*, 349 F.3d 1333, 1342 (Fed. Cir. 2003) and *In re Royka*, 490 F.2d 981, 985 (CCPA 1974)).

Consequently, Appellant respectfully submits that since the Examiner has not established a *prima facie* case of obviousness for the reasons discussed above, claims 3 and 4 are not obvious over Drexler and Falk.

In view of the above, the Examiner erred in rejecting claims 3 and 4 under 35 U.S.C. § 103(a) over Drexler and Falk.

VIII. CLAIMS APPENDIX

See attached Claims Appendix for a copy of the claims involved in this appeal.

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS APPENDIX

None.

CONCLUSION

For the reasons explained above, the rejections of claims 1-8 should be withdrawn.

In the event that the Patent and Trademark Office determines that an extension and/or other relief is required, Appellant petitions for any required relief, including extensions of time, and authorizes the Commissioner to charge the necessary amount due in connection with the filing of this document to Deposit Account No. 02-4800.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date May 13, 2009

By: /Brian N. Fletcher/
Brian N. Fletcher
Registration No. 51683

P.O. Box 1404
Alexandria, VA 22313-1404
703 836 6620

Customer No. 21839

VIII. CLAIMS APPENDIX

Claims involved in the appeal of U.S. Patent Application Serial No. 10/537,300:

1. A cryptographic method during which an integer division of a type $q = a \text{ div } b$ and/or a modular reduction of a type $r = a \text{ mod } b$ is performed, where q is a quotient, a is a number containing m bits, b is a number containing n bits, with n less than or equal to m and b_{n-1} is non-zero, b_{n-1} being the most significant bit of the number b , comprising the steps of masking the number a by a random number p before performing the integer division and/or the modular reduction, and generating encrypted or decrypted data in accordance with a result of the division and/or modular reduction.

2. A method according to claim 1, wherein, in order to mask the number a , b times the random number p ($a \leftarrow a + b * p$) is added to the number a .

3. A method according to claim 1 wherein, after having performed an integer division, the contribution made by the random number p is taken away from the result of the integer division.

4. A method according to claim 3, wherein, in order to take away the contribution made by the random number p , said random number p is subtracted from the result of the integer division.

5. A method according to claim 1, wherein the random number p is modified at each implementation of the method.

6. A method according to claim 1, wherein the random number p is modified after a predetermined number of implementations of the method.

7. An electronic component comprising means for implementing a method according to claim 1, said means comprising a plurality of registers for storing the numbers a and b .

8. A chip card comprising a component according to claim 7.

IX. EVIDENCE APPENDIX

None

X. RELATED PROCEEDINGS APPENDIX

None